UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/603,562	06/24/2003	Branislav N. Mcandzija	15685P207	5500

45222 7590 10/18/2006

ARRAYCOMM/BLAKELY
12400 WILSHIRE BLVD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030

EXAMINER	
ARANI, TAGHI T	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 10/18/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/603,562	MEANDZIJA ET AL.	
	Examiner	Art Unit	
	Taghi T. Arani	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 July 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16,18-21 and 23-32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4,7-10,13,14,18,19,23-26,29 and 30* is/are rejected.

7)☐ Claim(s) *5,6,11,12,15,16,20,21,27,28,31 and 32* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Taghi T. Arani
Primary Examiner
Art Unit 2131
10/14/06

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *08/08/2006*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 17, 22 and 33 have been cancelled.

Claims 1-16, 18-21, 23-32 have been examined and are pending.

Response to Amendment

2. Applicant's amendment filed 07/28/2006 necessitated the new ground(s) of rejection presented in this Office action. Therefore, applicant's arguments with respect to claims 1-16, 18-21, 23-32 have been considered but are moot in view of the new ground(s) of rejection.

Accordingly, THIS ACTION IS MADE FINAL. See MPEP 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claim1-3, 7-9, 13, 18, 23-25 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over prior art of record, US patent 6,189,098 to Kaliski, Jr., and further in view of US patent 6,886,095 to Hind et al. (hereinafter "Hind").

As per claims 1, 7, 23, Kaliski, Jr. teaches a method and a machine-readable medium storing instructions that, when performed by a user terminal of a wireless access network, the method (operations) comprising (Abstract, Fig. 1, Fig. 3A and associated texts)):

scrambling a user terminal certificate using a shared secret to be known only by the user terminal and an access point of the wireless access network (col. 4, lines 39-55, where the client's certificate (CERT-C) is retrieved from memory, EPROM 3, encrypted (scrambled) with the secret session key KSS (shared secret key), the scrambled user terminal certificate including a user terminal public key which corresponds to a user terminal private key (col. 10, lines 30-50, i.e. concatenating a time-varying value with the user terminal certificate (which includes user terminal public key which corresponds to a user terminal private key) and encrypting the result using the shared secret);

sending a message to the access point, the message including the scrambled user terminal certificate (col. 4, lines 53-55, message {CERT-TC}KSS is sent to server at 108 (access point).

Kaliski, Jr. does not teach but Hind teaches generating authenticator string including data encrypted with the user terminal private key; and sending the authenticator string to the access point (col.12, lines 42-55).

Therefore, It would have been obvious to one of ordinary skill in the art to modify the teachings of Kaliski, Jr. to include an authenticator string demonstrating possession of the user's s terminal private key as taught by hind with a motivation that an imposter would not be able to impersonate the user terminal of Kaliski, Jr. by replaying the certificate in transmission (hind, col. 12, lines 55-62).

As per claims 2, 8 and 24, Kaliski, Jr. teach the method, the machine-readable medium and user terminal of claims 1, 7 and 23 respectively, further comprising generating the shared

secret and providing the shared secret to the access point (col. 4, lines 43-46, the client also generates a random secrete session key (KSS) employing a number generator).

As per claims 3, 9 and 25, Kaliski, Jr. teaches the method of claims 1,7 and 23 respectively, wherein providing the shared secret to the access point comprises encrypting the shared with an access point public key (col. 4, lines 46-51, a time-varying TS and the secret session key KSS are concatenated and the result is encrypted with the server's public key PUBserv and the encrypted message is sent to the server).

As per claims 13, 18 and 29, Kaliski, Jr. teaches a method, a machine-readable medium performed by an access point of a wireless access network, the method (operations) comprising (Figs. 2 and 3B and associated texts):

receiving a message from a user terminal of the wireless access network, the message containing a shared secret encrypted with an access point public key(col. 4, lines 56-57), and a user terminal certificate scrambled using the shared secret, the scrambled user terminal certificate including a user terminal public key which corresponds to the user terminal private key (col. 10, lines 30-50, i.e. concatenating a time-varying value with the user terminal certificate (which includes user terminal public key which corresponds to a user terminal private key) and encrypting the result using the shared secret);

decrypting the shared secret using an access point private key; and

unscrambling the user terminal certificate using the decrypted shared secret (col. 4, lines 58 through col. 5, lines 11).

Kaliski does not teach but Hind teaches an authenticator string authenticator including data encrypted with a user terminal private key and decrypting the authenticator string using the user terminal public key (Hind, col. 7, line 57 through col. 8, line 23, see also col. 6, lines 10-25).

It would have been obvious to one of ordinary skill in the art to modify Kaliski's certificate with Hind's user terminal certificate containing identification of user terminal and a user terminal public key corresponding to a user terminal private key, wherein the user terminal certificate is used to authenticate the user terminal with a motivation to couple Kaliski's certificate with both users of the terminal and the terminal in order to solve the prior art problems associated with users' certificates in enterprise situations where each application (user) as well as each device may require a different levels of security , requiring the ability to allow different levels of security accesses (Hind, col. 7, lines 12-24).

4. Claims 4, 10, 14,19 and 26 and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kaliski, Jr. and Hind as applied to claims 1, 7, 13, 18, 23 and 29 above, and further in view of Persson et al. (prior art of record), US patent 6,754,824 (hereinafter "Persson").

As per claims 4, 10 and 26, Kaliski as modified teaches the method, the user terminal and the machine-readable medium of claims 1, 7 and 23 respectively, except wherein scrambling the user terminal certificate using the shared secret comprises combining the user terminal certificate with a pseudo-random sequence generated by a linear feedback shift register initialized with a part of the shared secret.

However, in an analogous art, Persson is directed to telecommunications systems and methods wherein the identity of the transmitting node is verified by modulating the CRC code utilizing a sequence known only to the participating parties. The modified CRC is generated by both the transmitting node and the receiving node initializing a LFSR register by a common key known only to the participating nodes (i.e. a pseudo-random sequence generated by a linear feedback shift register initialized with a part of the shared secrete [Persson, col. 2, lines 5-23]).

Therefore, it would have been obvious to one of ordinary skill at the time the invention was made to employ the teachings of Persson within the modified method and system of Kaliski for combining Kaliski's certificate with a pseudo-random sequence generated by a linear feedback shift register initialized with a part of the shared secret in order to verify both the authenticity of the received certificate and the identity of transmitting node and to deter unauthorized party to replace the participating nodes if week encryption or no encryption is switched on after authentication (Persson, col. 1, lines 35-49).

As per claims 14, 19 and 30, while modified Kaliski teaches unscrambling the user terminal certificate using the decrypted shared secrete (col. 4, line 659 through col. 5, line 1), Kaliski does not teach wherein unscrambling the user terminal certificate using the shared secret comprises combining the scrambled user terminal certificate with a pseudo-random sequence generated by a linear feedback shift register initialized with a part of the decrypted shared secret.

However, in an analogous art, Persson is directed to telecommunications systems and methods wherein the identity of the transmitting node is verified by modulating the CRC code utilizing a sequence known only to the participating parties. The modified CRC is generated by

both the transmitting node and the receiving node initializing a LFSR register corresponding to common key known only to the participating nodes (i.e. a pseudo-random sequence generated by a linear feedback shift register initialized with a part of the decrypted shared secrete [Persson, col. 2, lines 5-23, see also col. 4, line 53 through col. 18]).

Therefore, it would have been obvious to one of ordinary skill at the time the invention was made to employ the teachings of Persson within the modified method and system of Kaliski for combining Kaliski's certificate with a pseudo-random sequence generated by a linear feedback shift register initialized with a part of the shared secret in order to verify both the authenticity of the received certificate and the identity of transmitting node and to deter unauthorized party to replace the participating nodes if week encryption or no encryption is switched on after authentication (Persson, col. 1, lines 35-49).

Allowable Subject Matter

4. Claims 5-6, 11-12, 15-16, 20-21, 27-28 and 31-32 objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Action is Final

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after

the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Taghi T. Arani whose telephone number is (571) 272-3787. The examiner can normally be reached on 8:00-5:30 Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Taghi T. Arani, Ph.D.
Primary Examiner
Art Unit 2131
10/14/06